Rousseau, le contrat social et le numérique à l'épreuve du déconfinement

Aujourd'hui, pour la première fois depuis plus d'un siècle, nous voici amenés à débattre de la modification ou du rééquilibrage de certains aspects de ce contrat social afin de faire face à une pandémie mortelle.

À l'heure du déconfinement, l'un des principaux défis à relever pour contrôler la propagation du coronavirus et réduire le risque d'une seconde vague d'infections est la recherche des contacts : il s'agit d'identifier les personnes et les groupes d'individus avec lesquels une personne porteuse du virus peut avoir été en contact.

Dans des circonstances normales, la simple idée de collecter des données issues des téléphones portables pour suivre en masse le déplacement de leurs utilisateurs sans leur consentement serait une hérésie, en totale contradiction avec de nombreux règlements sur le respect de la vie privée. Mais, bien sûr, une pandémie mondiale n'est pas vraiment une circonstance normale.

La recherche des contacts COVID-19 est particulière en ce sens qu'un anonymat complet n'est pas possible : il est nécessaire d'identifier nominativement les personnes porteuses du coronavirus. C'est ce que font déjà les systèmes de santé nationaux, qui suivent les cas COVID-19 et font tout ce qui est en leur pouvoir pour rechercher les personnes avec lesquels ces patients ont pu entrer en contact.

Et évidemment, pour nous qui travaillons dans le domaine IT, la question se pose forcément de savoir comment la technologie peut apporter son aide tout en ne violant pas fondamentalement les attentes légitimes de la population en matière de protection de la vie privée…

Vie privée et santé publique

Les gouvernements peuvent aisément utiliser ou accéder aux informations de localisation des téléphones portables sans le consentement de l'utilisateur. Seulement voilà : si l'on justifie l'accès à ces données dans ces circonstances particulières, dans quelles autres circonstances futures les gouvernements pourront-ils décider, unilatéralement, d'avoir recours à ces mêmes technologies ?

Il existe également des approches purement *opt-in* où les personnes qui souhaitent participer à la recherche de contacts peuvent télécharger une application. Mais il faut qu'un très grand nombre de personnes installe cette application pour que l'approche soit réellement efficace, et rien ne le garantit.

Google et Apple ont proposé une solution intermédiaire intéressante. Celle-ci s'appuie sur de nouvelles capacités dans les systèmes d'exploitation iOS et Android, utilisées spécifiquement pour permettre la recherche de contacts de proximité avec une certaine anonymisation intégrée.
Cette approche permet de limiter à l'essentiel la collecte et l'analyse des données.
Par exemple, le système utilisera les signaux Bluetooth, qui ont une portée limitée et ne peuvent servir qu'à déterminer la proximité relative d'autres appareils, tout en interdisant le suivi de la

localisation, qui permettrait selon une étude du MIT de stocker la position géographique absolue d'un appareil.

Lorsque ces capacités seront déployées, si elles sont activées par défaut, elles pourraient permettre aux applications qui s'appuieraient sur cette plateforme de fédérer plus d'utilisateurs et d'aboutir à des programmes de recherche de contacts plus efficaces.

Avec de telles informations, les gouvernements pourraient mener des campagnes de recherche plus précises, ce qui permettrait d'améliorer l'approche sociétale de la prévention, du confinement et de l'atténuation des effets non seulement du COVID-19, mais aussi d'autres pandémies futures.

Mais le mot clé ici est « pourrait ». Les défenseurs de la vie privée s'empressent de souligner qu'il n'y a aucun moyen de savoir avec certitude si ces données amélioreraient suffisamment l'efficacité de la recherche des contacts et permettraient de sauver de nombreuses vies. Mais il n'y a non plus aucun moyen de le savoir sans essayer !

Il reste toutefois qu'il sera probablement compliqué, même sous cette forme, de faire en sorte que les habitants d'un pays entier – sans parler de la planète entière – consentent à ce que leurs données soient ainsi utilisées.

La « corde d'Andon » adaptée au numérique

Pour autant, la possibilité que la technologie existante puisse nous protéger contre les pandémies est une promesse de santé publique trop importante pour ne pas l'explorer. La question est juste de savoir comment se prémunir des abus envers la confidentialité des données. Une piste de réponse consiste à reconnaître qu'il s'agit d'une circonstance extraordinaire et qu'elle doit être traitée comme telle.

De nombreuses industries ont déjà passé pas mal de temps à réfléchir à la manière de faire face aux situations d'urgence. Dans le domaine de l'automobile, par exemple, lorsqu'un problème survenait dans une usine Toyota, les employés étaient habilités à arrêter la chaîne de montage au premier signe d'un problème. Il suffisait pour cela de tirer sur la « corde d'Andon » afin que les chefs d'équipe et les travailleurs puissent se rassembler pour résoudre le problème et relancer la production en suivant des étapes formalisées.

Aujourd'hui, les gouvernements ont besoin d'un système similaire qu'ils peuvent utiliser à l'échelle du pays lorsqu'une urgence extrême l'emporte sur les préoccupations relatives à la vie privée. Adapté au numérique, un tel système devrait comporter trois éléments principaux :

1 – Un point d'instigation
Le protocole devrait indiquer les facteurs permettant de positionner la catastrophe sur un spectre – par exemple, le niveau le plus élevé serait si la survie de notre espèce était en danger.

2 – Un point de démarcation
Les limites de la vie privée doivent être réimposées après la désescalade. Cela devrait être fixé avec une date et une heure prédéfinie au début du processus d'alerte.

3 – Un point d'intimité.

Partout où des données supplémentaires sont collectées, elles doivent l'être si possible dans le respect de la vie privée. Des approches telles que le Private Kit du MIT, une application de recherche des contacts, permettent aux personnes infectées de partager leur piste de localisation avec les responsables de la santé, mais ces informations sont anonymisées et les données des patients sont stockées localement.

Il est nécessaire que les gouvernements explicitent clairement et publiquement comment ils entendent respecter les trois éléments ci-dessus, en mettant l'accent sur les mesures qu'ils prennent pour préserver la vie privée et sur la date exacte à laquelle ils prévoient de mettre fin à l'utilisation des données.

Car chaque fois qu'un gouvernement écorne le contrat social, il risque de perdre la confiance du public. Sans transparence sur les données ni critères formels liés à cette « corde d'alerte », il y aura un retour de bâton. Et cela se traduira probablement par le refus des citoyens de tout type de suivi des contacts – y compris encadré -, ce qui irait à l'encontre de l'objectif d'utilisation de ces données pour améliorer la santé publique.